

07-19-00

A

BOX PATENT APPLICATION
 Commissioner for Patents
 Washington, DC 20231

Attorney's Ref: LOCK/170/US
 Date: July 18, 2000

Sir:

Transmitted herewith for filing is the (X) utility () design patent application of
 Inventor(s): GARY E. LAVELLE and JAMES YUAN
 For: INTERNET BASED ACCESS POINT MANAGEMENT SYSTEM

JC675 U.S. PTO
 09/618516
 07/18/00

Enclosed are:

- (X) 5 sheets of (X) formal () informal drawings.
- (X) An Assignment of the invention to HARROW PRODUCTS, INC.
- () A certified copy of a _____ application.
- () An associate power of attorney.
- () A verified statement claiming small entity status.
- (X) A Declaration (Signed)
- () A preliminary amendment.

The filing fee has been calculated as shown below:

- () design application for () small entity = \$155 () not small entity = \$310
- (X) utility application

	<u>No. Filed</u>	<u>No. extra</u>	<u>Small Entity</u> <u>Rate</u>	<u>Fee</u>		<u>Not Small Entity</u> <u>Rate</u>	<u>Fee</u>
Basic Fee				\$345	OR		\$690.00
Total Claims	49	- 20 = 29	x 09 =		OR x	18 =	522.00
Indep. Claims	5	- 3 = 2	x 39 =		OR x	78 =	156.00
Multiple Dependent Claims Presented			+ 130 =		OR +	260 =	
			TOTAL =			TOTAL =	<u>\$1,368.00</u>

- (X) A check in the amount of \$ 1,368.00 to cover the Filing Fee is enclosed.
- () Please charge my Deposit Account No. 16-2563 in the amount of \$_____ to cover the filing fee. A duplicate of this sheet is enclosed.
- (X) The Commissioner is hereby authorized to charge any additionally required filing fees under 37 CFR 1.16 associated with this communication or credit any overpayment to Deposit Account No. 16-2563. A duplicate copy of this sheet is enclosed.
- () The Commissioner is hereby authorized to charge fees under 37 CFR 1.16 and 1.17 required during the pendency of this application and to credit any overpayment to Deposit Account No. 16-2563. A duplicate copy of this sheet is enclosed.

GUY D. YALE, Reg. No. 29,125
 Alix, Yale & Ristas, LLP
 750 Main Street
 Hartford, CT 06103-2721
 Telephone: (860) 527-9211

EXPRESS MAIL Mailing Label Number EL 610584078 US

I, Doti Ann Lewis, hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" Service under 37 CFR 1.10 on July 18, 2000 and is addressed to the Box Patent Application, Commissioner for Patents, Washington, DC 20231.

Doti Ann Lewis
 Doti Ann Lewis

INTERNET BASED ACCESS POINT MANAGEMENT SYSTEM

Background of the Invention

The present invention relates generally to networks for managing
5 operations of a system and, more particularly, the present invention
relates to network management systems for managing access control
systems.

Currently, access point management systems (APMS) typically
include a desktop computer having a database for managing various
10 access points such as a door or a locker. The administrator or operator
logs onto the desktop computer and performs management functions
such as assigning a user's access credentials, for example, card
identification or access codes, grouping users access privilege with a
respective access point and scheduling timed events such as a specific
15 time interval during which access points may be in an accessible or in
a lockout condition. For the stand-alone type of computer managed
opening the operator uses a portable device, e.g. a palm top computer,
to download the access information from the desktop computer and
travels to the specific access point to download the data to a controller.
20 The portable device may also retrieve data from the access point for
uploading back to the desktop computer. In the situation where the
access point is online, such as in the case of a network based computer
managed opening, the access information can be exchanged with the
controller of the access point without movement by the operator. In

LOCK/170/US

particular, the controller may be electronically connected to the desktop computer whereby operators may instantaneously modify operation of the access point without downloading or traveling to the access point.

A problem arises in that one or more administrators that are highly trained and experienced with computer hardware and software are required to handle and support each site. This is particularly so where the site is as large as a school or a university each of which typically has a relatively complex security system. For example, the facilities of a university may be spread across a number of buildings, each of which may include laboratories, cabinets and storage structures disposed therein to which various individuals may be authorized access on a specified basis. Accordingly sophisticated authorization systems may be required, for example, to grant general access to various groups of individuals or specific access to particular individuals themselves.

Each of the access points may include one or more locking devices, such as, for example, an electronic lock control mechanism which is integrated with a lock set of a door as described in U.S. Patent No. 5,640,863 to Frolov issued June 24, 1997, assigned to the present assignee hereof and entitled "Clutch Mechanism for Door Lock System".

Another suitable example, is described in U.S. Patent Application Serial No. 09/495,497 (attorney docket number LOCK/166/US) filed on February 1, 2000 and entitled "Anti-jam Locking Mechanism for

Electronic Security System also assigned to the present assignee hereof.

The entire contents of both references are hereby incorporated herein by reference.

Since the administrator has total control and responsibility of the data base management and maintenance, relatively large resources in terms of training, knowledge and experience are required to maintain these security systems. In addition, hardware upgrade and software changes may cause compatibility problems for the administrator. In addition, periodical data base maintenance including integrity checks and backups must be undertaken on an ongoing basis. Accordingly, the combined direct and indirect administrative and maintenance cost of these activities may be significant especially when one adds the cost associated with a number of facilities.

In view of the foregoing, a need has arisen for providing for an efficient centralized access point management system for managing a plurality of sites using essentially a single management system.

Summary of the Invention

Briefly stated, the invention in a preferred form is an internet based access point management system accessible by an internet web browser configured to communicate one or more requests for modifying operation of one or more computer managed openings located at one or

more facilities. The internet based access point management system includes at least one computer processor having a web server operative with at least one computer processor. The web server is configured to receive and respond to one or more requests communicated from one or more web browsers. A database server which is also operative with the at least one computer processor and an application server further operative with the at least one computer processor are also provided. The application server is configured to communicate with the web server and the database server for processing requests. The processing of requests includes formulating system commands in response to the requests. A communication link is configured to connect the application server and the one or more computer managed openings for communication therebetween. The communication includes system commands which modify operation of the one or more computer managed openings.

In accordance with another embodiment of the present invention, a method of managing an access control system for a facility, employing at least one computer managed opening is provided. The method comprises the steps of generating a request to modify operation of one or more computer managed openings which are stand-alone, network or modem based; communicating the request to a remote computer managed opening server; processing the request at the remote computer

managed opening server in order to generate an acknowledgement of the request and to generate one or more system commands; selecting the appropriate electronic format for the one or more system commands depending upon whether the one or more computer managed openings
5 are stand-alone, network or modem based; and communicating the one or more system commands to the appropriate computer managed opening for modifying operation thereof.

In accordance with one embodiment of the invention the step of generating a request comprises inputting data to a web browser; the
10 step of communicating the request comprises passing the request from the web browser to a web server over the internet; the step of processing is performed by an application server and comprises retrieving data concerning one or more computer managed openings from a data base; and the step of selecting the appropriate electronic
15 format is also performed by the application server and comprises selecting file transfer protocol for the system commands where the computer managed opening has a stand-alone type configuration and selecting electronic mail message format for the system commands where the computer managed opening is network or modem based.

20 An object of the present invention is to provide a distributed management system for managing a plurality of security systems located at multiple facilities.

Another object of the present invention is to provide a management system for access control systems which is efficient and reduces the maintenance and management costs for each facility.

A further object of the present invention to provide a
5 management system which may be operated without significant training and continuing education requirements for the facility operators.

Other objects and advantages of the invention will become apparent from the specification and the drawings.

10 **Brief Description of the Drawings**

Figure 1 is a schematic diagram of an internet based access point management system in accordance with one embodiment of the present invention;

Figure 2 is a schematic diagram of a controller connected to a
15 local gateway and input/output devices of a computer managed opening in accordance with the embodiment of Figure 1;

Figure 3 is a schematic diagram showing the interface between various components of a remote computer managed opening (CMO) server and the interface between the CMO server and user browser and
20 various components of a representative facility in accordance with the embodiment of Figure 1;

Figure 4 is a schematic diagram of the communication paths between various elements of a computer managed opening in accordance with the embodiment of Figure 1; and

Figure 5 is a schematic diagram of a relational database employed
5 in accordance with the embodiment of Figure 1.

Detailed Description of the Preferred Embodiments

An internet based access point management system (APMS) in accordance with an embodiment of the present invention is illustrated
10 generally at 10 in Figure 1. The internet based APMS 10 comprises a remote computer managed opening (CMO) server 12 that may be connected by a router 14 in a well known manner to the internet 16 via line 17. A first facility 18, second facility 20 and third facility 22 are connected to the internet via lines 24, 26 and 28, although, it will be
15 understood that wireless communication may instead be employed. It will also be understood that while facilities 18, 20 and 22 are illustrated as including different security configurations, e.g. networked versus non networked systems, as discussed in more detail below, one or more facilities having similar security configurations may be employed in
20 accordance with the present invention. Also, while multiple facilities are illustrated, a single facility having one particular security configuration

or multiple security configurations may be employed in accordance with this embodiment of the present invention.

As used herein the term access point refers to a location containing a selectively controllable opening such as a gate, door,
5 cabinet, etc.

As used herein the term locking device refers to an electronically controlled device for selectively locking an access point such as, for example, the device described in the previously incorporated U.S. Patent No. 5,640,863 and U.S. Application Serial Number 09/495,497
10 (attorney docket number LOCK/166/US).

As used herein the term computer managed opening (sometimes herein referred to as a CMO) refers to a computer, e.g. a desk top or lap top, either networked together with, or standing alone from, one or more locking devices each being connected to an access point and, as
15 described in more detail below, any electrical/electronic devices interconnecting the computer with the locking device.

The first facility 18 comprises computer managed openings 30 of the stand alone type each of which comprise an access point 32a, 32b and 32c, computer 36 and a locking device controller 38a, 38b and
20 38c. The computer 36 is used by an operator, as will be more fully described hereafter, in order to modify operation of the computer managed openings 30. In order to do so, the computer 36 includes a

web browser (not shown) for communicating in a known manner over the internet 16 with the remote CMO server 12. The web browser may be any commercially available program such as that sold under the trademark NETSCAPE by the Netscape Communications Corporation of Mountain View, California or the trademark EXPLORER by the Microsoft Corporation of Redmond, Washington. Once the operator has received data from the remote CMO server 12, the operator must download information from the computer 36 to a portable device (not shown) such as a palm top computer. Thereafter, the operator may travel from an operator location 40 to the locking device controllers 38a, 38b and 38c depending upon the particular locking device controller to be updated.

The second facility 20 comprises computer managed openings 41 which are network based and each include an access point 42 and 44, CMO network 46 and a local gateway 48. The local gateway 48 is electrically connected between the CMO network 46 and an intranet 50.

Referring now also to Figure 2, the local gateway 48 is connected between a controller 52 and the internet 16 and serves as an interface between the controller and the internet, as will be described in more detail hereafter. The controller 52 is, in turn, connected to an access point such as 42, 44 and comprises a printed circuit board 54 having an embedded microprocessor 56, a clock 58, non-volatile memory 60 and a transceiver 62. The embedded microprocessor 56 may be obtained

commercially and a suitable microprocessor includes that sold under the name "The Neuron" by the Echelon Corporation of Palo Alto, CA and that sold under the name "Nett 5" by Net Silicon of Waltham, MA. The non-volatile memory 60 may be for example EPROM or EEPROM and
5 contains, e.g., data base information usable for selectively authorizing access through each access point for each individual associated with the facility. The transceiver 62 communicates with the CMO network 46 as is well known. A reset switch 64 and service module connector 66 may also be provided in a known manner. A power supply 68 is
10 provided for energizing the controller 52.

Input/output ports 70 are provided for communicating with devices 72, e.g., a card reader and/or a locking device such as an electromagnetic lock or electric strike which controls opening of, for example, access points 42, 44 which are illustrated as doors. In
15 particular, door locks, cabinet locks or any openings that need a proper credential to verify the privilege of passage "or accessibility" may be connected to the controller 52. The microprocessor 56 functions to, among other things, effect locking or releasing of a locking device in response to a users' credential, a prescheduled time, a predefined event
20 or even an emergency situation such as in the event of a fire. An onboard database contained in the nonvolatile memory 60 allows the controller 52 automatically to take such actions. The controller 52 is

also able to communicate with the local gateway to extend its functions and update its firmware contained in non-volatile memory 60. Each controller 52 may be identified by a unique logical address in the local CMO network 46.

5 Referring again only to Figure 1, an operator computer work station 74 is provided which includes a web browser (not shown) for communicating in a known manner through a fire wall 76 and over the internet 16. The web browser may be any commercially available program such as is discussed above. It will be appreciated that the fire
10 wall 76 may comprise a computer system running a program which prevents passage of undesirable communication between the operator workstation 74 and internet 16. A mail server 78 is connected to the internet 16 and communicates with the local gateway 48 and the computer workstation 74 and the internet 16. Optionally, it will be
15 appreciated that a mail client may be substituted for the mail server 78 where appropriate. The mail server 78 may be disposed on the same computer system as the fire wall 76 and this computer system may also support the intranet 50. Optionally, depending on, e.g., the connection speed supportable by the lines 17 and 26, the mail server 78 may be
20 used to support the firewall 76 and/or intranet 50.

The third facility 22 comprises computer managed openings 78 which are modem based and which include an access point 80, 82, and

84. A CMO network 86 which is connected to a local gateway 88 which communicates with the CMO network and a modem 90. An electronic mail server 92 (or optionally a mail client similar to that discussed above) communicates with the modem 90 (via another 5 modem (not shown)) and internet service provider (ISP) 94. The ISP 94 and mail server 92 may be connected by an intranet 93 and the ISP is in communication with the internet 16 via line 28.

The remote CMO server 12 comprises a mail server 96, a database server 98, a web server 100 and an application server 102. 10 While each of the mail server 96, database server 98, web server 100 and application server 102 are illustrated as being disposed on separate computer processing units. It will be appreciated that all of them may be disposed on one computer processing unit.

The mail server 96 manages incoming and outgoing mail in the 15 respective account directory for each administrator. Outgoing mail is deposited by the application server 102 and is sent to the destination local mail server, e.g., local mail server 78, as soon as it arrives. Incoming mail may be stored in a directory for the application server to pick up. The mail server 96 also serves to formulate and communicate 20 electronic mail to be sent to a particular destination. In particular, a unique e-mail address is assigned to each local mail server 78 and/or local gateway 48 whereby electronic messages may be communicated

between the mail server 96, local mail server, local gateway and thereafter to the controller 52.

With additional reference to Figure 3, the web server 100 functions to communicate over the internet with a client browser 104 which may be incorporated, for example, in the work station 74. The web server 100 is commercially available from the Apache Software Foundation of Forest Hill, MD under the name "Apache Web Server" and handles client requests such as from a client administrator operating a client browser 104. The web server 100 responds to the client browser 104 after communication with the application server 102. In particular, a database server 98 stores various information, described in more detail below, which the application server 102 uses in responding to the web server 100 and formulating system commands for passage to the mail server 96. In this way, the application server 102 communicates with the web server 100 concerning client requests, parses them and then processes the result and/or prepares an acknowledgment for return to the web server 100 which in turn provides this information to the client browser 104. As discussed above, the client browser 104 may be any suitable browser as is well known. In this manner, the client may contact the web server 100 through the client browser 104 in order to perform management functions such as assigning users access

credentials which may include preparing an ID card or granting particular access codes.

It will be appreciated that the application server 102 may comprise a software program in a dedicated computer system.

5 The application server 102 is a coordinator between the service providers and helps the web server 100 to parse and dispatch administrator requests to process and to assemble the response for the web server. The application server 102 decides data flow either to be processed by the data base server 98 or to be returned by the web
10 server 100 through the mail server 96. The application server 102 picks up the incoming mail from the mail server 96 for proper processing. It may authenticate client access if a proxy server is not present. Then application server 102 invokes the database server 98 or other components to process the request and prepare an acknowledgement
15 which is communicated via the web server 100 to the administrator through the web browser 104.

 The application server 102 also prepares one or more system commands during processing of the request for modifying the operation of one or more of the computer managed openings. Once the
20 processing of a request has been completed, the application server 102 determines whether the system commands are to be communicated to either the web server 100 or the mail server 96. In the situation where

the computer managed opening is of the stand-alone type, such as illustrated in facility 18, the application server 102 may format the system commands in, e.g., file transfer protocol for transfer by the web server 100 to the client browser 104 for downloading by the operator
5 as discussed previously. Otherwise, where the computer managed opening to be modified is network or modem based and includes a local gateway, the application server 102 may, e.g., formulate an electronic mail message based on the system commands to be communicated by the mail server 96 to a local mail server such as local mail server 78.
10 Examples of the format of those messages are discussed in detail hereafter.

Referring now to Figures 1 and 4, the local gateway 48 may comprise a gateway server component 106 and an electronic mail agent component 108. The gateway server component 106 communicates
15 with the controller 52 via a communications format such as is illustrated in Figure 5. In particular, the communications format preferably comprises a byte string from byte 0 to byte 31 where byte 0 is the command identification which may be represented by numerical designation from 0 to 255. The command identification is useful for
20 identifying a particular command such as 03 which may be used to identify a command to update a user's record. An example list of commands represented by numerical designation is as follows.

	01	Delete the user database
	02	Read on user record
	03	Update one use record
	04	Verify on user record
5	05	Update configuration
	06	Report configuration
	07	Get version
	08	Clear network variable
	09	Update time
10	10	Read time
	11	Onboard Event History Report
	12	Onboard Event History Resume
	13	Onboard Event History Clear
	14	Request audit trail
15	15	Search Server database
	16	Reserved
	17	Signature report
	18	Signature reset
	19	Release point
20	20	Door status
	21	Number of bytes for onboard database
	22	Read next time schedule
	23	Read next time zone
	24	Report current time schedule
25	25	Report current time zone
	26	Update single time zone
	27	Update single time schedule
	28	Update single holiday
	29	Read I/O buffer
30	30	Start system status poll
	31	Stop system status poll
	32	Credential matched
	33	Lost credential protection
	34	Remote Toggle
35	35	Packet Acknowledge
	36	Update user expiration date
	37-255	Reserved for future use

Byte 1 provides the length of a command and bytes 2-31 comprise the
40 command. The command may, for example, update the database of the

computer managed opening controller 52 to include an additional user and the additional user's access points.

An example of a command string useful in accordance with one embodiment of the present invention is provided in TABLE I which
5 includes the following message in hexadecimal format.

TABLE I

	Byte 0:	03 (update user record)
	Byte 1:	0A (user record size)
10	Byte 2-3:	008A (two bytes record number)
	Byte 4,5,6:	030A08 (three bytes credential number)
	Byte 7,8:	03E1 (two bytes attribute- application specific)
15	Byte 9,10,11:	07EF83 (three bytes expiration date- application specific)

The electronic mail agent component 108 may comprise either software or firmware and interfaces with the gateway server component
20 for translation of system commands from electronic mail messages into the, for example, LonTalk™ format, as exemplified above. The e-mail

agent component 108 also functions to communicate messages in e-mail format with the local mail server 78.

The local CMO gateway 48 comprises two network interface cards NICs (not shown). One of the NICs is connected with the CMO network 46 (Figure 1) the other of which is connected in circuit with a local area network, i.e., intranet 50. It will be appreciated that the local gateway 88 would not require a second network interface card as it is connected to the modem 90. The local gateway 48 communicates with the remote CMO server 12 via the local mail server 78. The local gateway 48 may optionally also serve as an extended database for each of the controllers 52. In particular, when e.g., a user credential, such as a user ID, is presented at the controller 52 a data base lookup is required to see if the credential is valid. The controller 52 will preferably query its own local database first. If the credential is not found locally, the controller 52 will advantageously request the gateway 48 to query the extended database. The gateway 48 will then respond to the controller 52 based on the results of the query.

The extended data base of the gateway 48 may be configured to maintain a log of transactions by controller 52. When access is granted at the controller 52, a transaction record is passed to the gateway 48.

The gateway records the entry in the extended database along with a time and date stamp. This database serves as a log file or audit trail

record providing access history. This access history can then be queried to compile access history either by access point or by user. If, for example, the network 46 is not operational, and the controller 52 is unable to communicate with the gateway, the audit trail entry is stored
5 locally in the controller database. The gateway 48 will then collect this information from the controller 52 and append it to the extended database when network 46 operation is restored.

In order to prevent any security breaches in the internet based access point management system 10, the local gateway 48 is
10 programmed to communicate only with the electronic mail server 78 and to achieve this result provides a polling function of the electronic mail server. To further secure the internet based access point management system 10, the electronic mail communicated between mail server 96 and mail servers 78 and 92 may be encrypted with a known encryption
15 method, such as in accordance with the data encryption standard (DES). To achieve this result, the mail servers 78, 92 and 96 may each contain encryption programs.

In the case of facility 22, a modem 90 polls the mail server 92 on a regular basis in order to obtain any e-mail messages. This also
20 reduces any long distance telephone charges.

The format of representative electronic mail messages may be as provided in the following TABLE II.

TABLE II

E-mail format from remote CMO server to local CMO gateway

5 Subject: indicates an internal defined message index
 identifier (uniquely numbered message)
 Contents: empty space
 Files Attached: at least one command file and one or more
 database table files (e.g. a new or revised time
 zone table).
10 Encryption: all attached files with predetermined,
 commercially available methods.

Format of the command file sent to local CMO gateway

15 It is a consecutive byte string without delimiter.
 Byte 0-1 : random number transaction ID to be used for
 acknowledgment.
 Byte 2-3 : number of commands in this byte string.
 Byte 4-end : command body.

Command body

 Byte 0-1 : the length of the command body
 Byte 2-3 : command ID
25 Byte 4-6 : CMO identification (000-999)
 Byte 7 : CMO sub ID ('A', 'B', 'C', or 'D').
 Byet 8-end : one or more command parameters.

E-Mail format from local CMO gateway to the administrator (or remote servers)

30 Subject : transaction ID from the command file if
 acknowledgment.
 Contents : predefined success or failure message.
35 Files attached : one or more database table files or a single
 record reporting a transaction if controlled in real
 time.
 Encryption : all attached files.

40 It will be understood that while the preferred embodiment
 provides for the communication between the remote CMO 12 and local

gateway 48, 88 via an internet electronic mail format, other formats may be employed as well, such as file transfer protocol (FTP). To achieve this, a file transfer protocol (FTP) server (not shown) may be used in connection with the remote CMO server 12. The FTP server
5 may be used to directly download or upload database information without invoking a mail server. For example, the stand-alone CMO has no gateway to upload onboard database automatically. Therefore, the operator downloads data to the CMO right after the data has been sent to the browser for varying the operation of a CMO. Data can be directly
10 downloaded to a portable device to program the CMO as discussed above. In this situation using an FTP server is more efficient since once the data has been transferred to the web hardware at the web browser, it is in position to be handled by the administrator. A proxy server may also be provided for enhanced security in order to improve the
15 performance by preventing direct access to the data bases. These servers may reside on the same computer running multiple processes or on separate computers and connected in a network fashion.

A security administrator's tool for a given facility is, as discussed above, a standard web browser running on a work station such as work
20 station 74 or any portable computer having internet access. The administrator thus need not perform updates on software or computer components. Instead, the maintenance is handled by off-site centralized

highly skilled staff which performs maintenance for numerous other facilities. User training is minimal for the administrator since the standard web browser is the main interface. The administrator may assign dozens or hundreds of users with different access privileges for use with various CMOs.

With reference to Figure 5, the database server 98 comprises a remote CMO database 110 which may be organized at 112 into three main categories, including a user database 114, an access type database 116 and an access point database 118. The user database 114 encompasses a hierarchy of data and relationships for defining user group layers 120 such as, in a university setting, students, employees and security staff wherein each group layer has a different access requirement, groups 122 such as students and users 124. It will be appreciated that each of the foregoing are related together by object and collection, as noted in the key 125 of Figure 5. The users 124 are also related by access type 116, for example, card reader or data pad. The group 122 is related to both users 124 and point interface 126. The access type 116 is related to reader 128 which refers to particular card readers, for example. The access points 118 relate to point groups 130 and particular points 132. The point groups, which comprise a collection of access points, may, for example, define various proximal access points or common entranceways for a dormitory. The particular

point 132, which may be a room within the dormitory, is related to the CMO type 134 which refers to whether the CMO is a stand-alone, network or modem based. It will be understood that the group interface 136 interacts with the point interface 126 through dynamic binding
5 during the export of files to the particular CMO's.

Operators 138 provide a listing of authorized administrators for each facility, e.g., a particular operator may be a lock and associated equipment installer. Accordingly this operator may have authority to add access points to the system, but no authority to modify user access
10 privileges. Another operator may be a human resource manager who can grant or modify access privileges but can not add or remove access points. Operators 138 are related to user group layers 140 which are related to particular groups 142, and the operators are also related to particular point groups 144 and points 146. The function of the local
15 gateways 148 is to provide a database containing the unique address and data associated with each local gateway as discussed above. The local gateways 148 are also related to particular CMO types 134. CMO types in turn 134 are related to readers 128 particular configurations 150 and time management 152, e.g., for varying the opening and
20 closing times.

With reference to Figures 3 and 4, the database server 98 works with the application server 102 to manage the database for various

clients through the web server 100, the gateway 88, the mail server 96 and the individual CMO through the gateway.

The data base server 98 preferably manages operations of each individual gateway and CMO and may, for example, store or access the following information. Software components such as for supporting a magnetic stripe card reader (see devices 72 of Figure 2) or for a component supporting a network protocol. A configuration database having, e.g., the internet protocol address of a particular gateway, a table of devices which are allowed to communicate with a particular gateway, the number and type of CMOs connected to a particular gateway and their addresses, the size of an access history log of a gateway and when it should be purged, etc. Individual CMO identification and firmware such as the latest version of firmware for a CMO or the particular configuration of a CMO, e.g., whether the CMO includes a magnetic stripe reader with an onboard memory for 1000 users, no time zone capability, etc. Gateway and controller onboard databases which may include a transaction log for an access point, the user list for the access point, the time schedule, etc.

While the present invention has been described in connection with what are presently considered to be the most practical and preferred embodiments, it is to be understood that the present invention is not limited to the disclosed embodiments. Rather it is intended to

cover all the various modifications and equipment arrangements included within the spirit and scope of the appended claims. For example, the mail components may be implemented with FTP instead of electronic mail format and/or CMO network protocols may be replaced with
5 embedded Transmission Control Protocol/Internet Protocol (TCP/IP) protocols.

What is claimed is:

1. An internet based access point management system accessible by at least one internet web browser configured to communicate one or more requests comprising modifying operation of one or more computer managed openings located at one or more facilities, the internet based access point management system comprising:

at least one computer processor;

a web server operative with the at least one computer processor and the web server being configured to receive and respond to one or more requests communicated from the at least one web browser;

a database server operative with the at least one computer processor;

an application server operative with the at least one computer processor and being configured to communicate with the web server and the database server for processing requests, the processing of requests comprising formulating one or more system commands in response to the requests; and

a communication link configured to connect the application server and the one or more computer managed openings for communication therebetween, the communication link comprising the one or more system commands which modify operation of the one or more computer managed openings.

2. The internet based access point management system of claim 1 wherein:

the one or more computer managed openings each comprise an access point each connected to a controller;

the communication link comprises:

a mail server operative with the at least one computer processor and being configured for communication of electronic messages in electronic mail format over the internet;

a local mail server or mail client operative with another computer processor and being configured to receive the electronic messages in electronic mail format over the internet from the mail server; and

a local gateway configured to communicate with the local mail server and the controllers; and

the application server is configured to incorporate system commands into electronic messages in electronic mail format and to communicate with the mail server.

3. The internet based access point management system of claim 2 wherein each controller comprises:

a power supply;

a transceiver for communication with the local gateway;

a processor energized by the power supply and connected in circuit with the transceiver;

non-volatile memory connected in circuit with the processor;

a clock connected in circuit with the processor;

an input port for receiving user input; and

an output port for connection to a locking device, the locking device being mechanically connected to the access point.

4. The internet based access point management system of claim 1 wherein the system commands modify operation of the one or more computer managed openings in order to perform at least one of the functions selected from the group consisting of assigning a user's access credentials, grouping a user's access privilege with a respective access point and scheduling time events.

5. The internet based access point management system of claim 1 wherein the processing of requests by the application server also comprises assembling a response for communication to the web server.

6. The internet based access point management system of claim 2 wherein the database server stores one or more of the following: individual local gateway electronic mail address, software components,

gateway configuration database, individual computer managed opening identification, CMO firmware, CMO configuration and gateway and controller onboard databases.

7. The internet based access point management system of claim 6 wherein the database comprises:

a user database comprising user group layers, user groups related to particular user group layers and users related to particular user groups;

an access type database comprising readers;

an access point database comprising access point groups with particular access points related thereto and to a computer managed opening type;

an operator database comprising operators being related to user group layers and particular user groups, the operators also being related to access point groups and access points;

a local gateway database comprises computer managed opening type; and

wherein the users are related to a particular access type and the user groups are related to a particular access point, the computer managed opening type is related to particular readers, configuration

database and time management of each access point and/or access point grouping.

8. The internet based access point management system of claim 2 wherein the local gateway comprises a gateway server component and an electronic mail agent component.

9. The internet based access point management system of claim 2 wherein the local gateway converts the electronic messages from the electronic mail format to LonTalk™ protocol.

10. The internet based access point management system of claim 2 wherein the local gateway converts the electronic messages from the electronic mail format to another format comprising a command string comprising a command identification, a length of one or more commands and at least one command.

11. The internet based access point management system of claim 2 wherein the local gateway further comprises an encryption/decryption device for encrypting/decrypting the electronic messages in electronic mail format and further comprising:

an encryption/decryption server operative with the at least one computer processor for encrypting/decrypting the electronic messages in electronic mail format.

12. The internet based access point management system of claim 2 wherein the electronic messages in electronic mail format comprise:

a subject comprising a message index; and

attached files comprising at least one command file and at least one database table file.

13. The internet based access point management system of claim 12 wherein the local gateway further comprises an encryption/decryption device for encrypting/decrypting at least one database table file and/or at least one database table file and further comprising:

an encryption/decryption server operative with the at least one computer processor for encrypting/decrypting at least one command file and/or at least one database table file.

14. The internet based access point management system of claim 13 wherein the command file comprises a consecutive byte string absent delimiters.

15. The internet based access point management system of claim 14 wherein the consecutive byte string comprises a transaction identification, a number of commands in the byte string and a command body.

16. The internet based access point management system of claim 15 wherein the command body comprises a length of the command body, a command identification, computer managed opening identification, computer managed opening sub-identification and at least one command parameter.

17. The internet based access point management system of claim 2 wherein the one or more computer managed openings are configured to generate reply messages which are converted into electronic mail format by the local gateway.

18. The internet based access point management system of claim 17 wherein the electronic mail format of the reply messages comprises:

- a subject which comprises at least one of a transaction identification or a message index;

- a contents which comprises a predefined success or failure indication; and

attached files comprising at least one database table file.

19. The internet based access point management system of claim 18 wherein the local gateway further comprises an encryption/decryption device for encrypting/decrypting at least one database table file and/or at least one database table file and further comprising:

an encryption/decryption server operative with the at least one computer processor for encrypting/decrypting at least one command file and/or at least one database table file.

20. The internet based access point management system of claim 1 wherein the at least one computer processor comprises three computer processors and wherein each of the web server, database server and application server each are operative with a separate one of the three computer processors.

21. An internet based access point management system at least a part of which resides on a computer readable medium and is accessible by at least one internet web browser configured to communicate one or more requests comprising modifying an operation of one or more computer managed openings located at one or more facilities, the internet based access point management system comprising:

a web server configured to receive and respond to one or more requests communicated from the at least one web browser;

a database server;

an application server configured to communicate with the web server and the database server for processing requests, the processing of requests comprising formulating one or more system commands in response to the requests; and

a communication link configured to connect the application server and the one or more computer managed openings for communication therebetween, the communication comprising the one or more system commands which modify operation of the one or more computer managed openings.

22. The internet based access point management system of claim 21 wherein:

the one or more computer managed openings each comprise an access point each connected to a controller;

the communication link comprises:

a mail server operative with the at least one computer processor and configured for communication of electronic messages in electronic mail format over the internet;

a local mail server or mail client operative with another computer processor and configured to receive the electronic messages in electronic mail format over the internet from the mail server; and

a local gateway configured to communicate with the local mail server and the controllers; and

the application server is configured to incorporate system commands into electronic messages in electronic mail format and to communicate with the mail server.

23. The internet based access point management system of claim 22 wherein each controller comprises:

a power supply;

a transceiver for communication with the local gateway;

a processor energized by the power supply and connected in circuit with the transceiver;

non-volatile memory connected in circuit with the processor;

a clock connected in circuit with the processor;

an input port for receiving user input; and

an output port for connection to a locking device, the locking device being mechanically connected to the access point.

24. The internet based access point management system of claim 22 wherein the local gateway comprises a gateway server component and an electronic mail agent component.

25. The internet based access point management system of claim 24 wherein the local gateway converts the electronic messages from the electronic mail format to another format comprising a command string comprising a command identification, a length of one or more commands and at least one command.

26. The internet based access point management system of claim 22 wherein the electronic messages in electronic mail format comprise:

a subject comprising a message index; and

attached files comprising at least one command file and at least one database table file.

27. The internet based access point management system of claim 26 wherein the local gateway further comprises an encryption/decryption device for encrypting/decrypting at least one command file and/or at least one database table file and further comprising:

an encryption/decryption server for encrypting/decrypting at least one command file and/or at least one database table file.

28. The internet based access point management system of claim 27 wherein the command file comprises a consecutive byte string absent delimiters.

29. The internet based access point management system of claim 28 wherein the consecutive byte string comprises a transaction identification, a number of commands in the consecutive byte string and a command body.

30. The internet based access point management system of claim 29 wherein the command body comprises a length of the command body, a command identification, computer managed opening identification, computer managed opening sub-identification and at least one command parameter.

31. The internet based access point management system of claim 22 wherein the one or more computer managed openings are configured to generate reply messages which are converted into electronic mail format by the local gateway.

32. The internet based access point management system of claim 31 wherein the electronic mail format of the reply messages comprises:

a subject which comprises at least one of a transaction identification or a message index;

a contents which comprises a predefined success or failure indication; and

attached files comprising at least one database table file.

33. The internet based access point management system of claim 32 wherein the local gateway further comprises an encryption/decryption device for encrypting/decrypting at least one database table file and/or at least one database table file and further comprising:

an encryption/decryption server operative with the at least one computer processor for encrypting/decrypting at least one command file and/or at least one database table file.

34. An internet based access point management system accessible by at least one internet web browser communicating one or more requests for modifying operation of one or more computer managed openings located at one or more facilities, comprising:

at least one computer processor;

a web server operative with the at least one computer processor and configured to receive and respond to one or more requests from the at least one web browser;

a database server operative with the at least one computer processor; and

an application server operative with the at least one computer processor and configured to communicate with the web server and the database server for receiving and processing commands, the processing of commands comprising formulating one or more system commands for communication to the web browser by the web server.

35. The internet based access point management system of claim 33 wherein the one or more computer managed openings each comprise an access point connected to a controller and further comprising:

a file transfer protocol server operative with a computer processor and configured to communicate with the web browser for converting the system commands into a format compatible with that used by access points and for downloading the system commands to a portable device for transfer to a particular controller.

36. An internet based access point management system at least partially residing on a computer readable medium and being accessible

by at least one internet web browser communicating one or more requests for modifying operation of one or more computer managed openings located at one or more facilities, comprising:

a web server operative with the at least one computer processor and configured to receive and respond to one or more requests from the at least one web browser;

a database server; and

an application server being configured to communicate with the web server and the database server for receiving and processing commands, the processing of commands comprising formulating system commands for communication to the web browser by the web server.

37. The internet based access point management system of claim 36 wherein the one or more computer managed openings each comprise at least one access point and further comprising:

a file transfer protocol server operative with a computer processor and configured to communicate with the web browser for converting the system commands into a format compatible with that used by the access points and for downloading the system commands to a portable device for transfer to a particular controller.

38. A method of managing an access control system for a facility, employing at least one computer managed opening, said method comprising the steps of:

generating a request to modify operation of one or more computer managed openings which are stand-alone, network or modem based;

communicating the request to a remote computer managed opening server;

processing the request at the remote computer managed opening server in order to generate an acknowledgement of the request and to generate one or more system commands;

selecting the appropriate electronic format for the one or more system commands depending upon whether the one or more computer managed openings are stand-alone, network or modem based; and

communicating the one or more system commands to the appropriate computer managed opening for modifying operation thereof.

39. The method of claim 38 wherein:

the step of generating a request comprises inputting data to a web browser;

the step of communicating the request comprises passing the request from the web browser to a web server over the internet;

the step of processing is performed by an application server and comprises retrieving data concerning one or more computer managed openings from a data base; and

the step of selecting the appropriate electronic format is also performed by the application server and comprises selecting file transfer protocol for the system commands where the computer managed opening is stand-alone based and selecting electronic mail message format for the system commands where the computer managed opening is network or modem based.

40. The method of claim 39, wherein:

the step of communicating the one or more system commands comprises:

communicating the system commands in file transfer protocol to the web server for communication to the web browser where the computer managed opening is stand-alone, whereupon an administrator may download and transfer the system commands to a controller; and

communicating the system commands to a mail server in electronic mail message format for communication thereof to a local mail server, the local mail server communicating the system commands to a

local gateway which translates the system commands into another format for communication to one or more controllers.

41. The method of claim 40 wherein the local gateway translates electronic mail message format into a command string comprising a command identification, a length of one or more commands and at least
5 one command.

42. The method of claim 40 wherein the electronic messages in electronic format comprises:
a subject comprising a message index; and
10 attached files comprising at least one command file and at least one database table file.

43. The method of claim 42 further comprises the steps of encrypting and decrypting the command file and/or the data base table file.
15

44. The method of claim 43 wherein the command file comprises a consecutive byte string absent delimiters.

45. The method of claim 44 wherein the consecutive byte string comprises a transaction identification, a number of commands in the consecutive byte string and a command body.

5 46. The method of claim 45 wherein the command body comprises a length of the command body, a command identification, computer managed opening identification, computer managed opening sub-identification and at least one command parameter.

10 47. The method of claim 40 further comprising the step of generating reply messages by the computer managed opening and the reply messages being in electronic mail format.

48. The method of claim 47 wherein the electronic mail format of the
15 reply messages comprises:

a subject which comprises at least one of a transaction identification or a message index;

a contents which comprises a predefined success or failure indication; and

20 attached files comprising at least one database table file.

ABSTRACT

An internet based access point management system is accessible by at least one internet web browser configured to communicate one or more requests for modifying operation of one or more computer managed openings located at one or more facilities. The internet based access point management system includes at least one computer processor having a web server operative with the at least one computer processor. The web server is configured to receive and respond to one or more requests communicated from the at least one web browser. A database server which is also operative with the at least one computer processor and an application server further operative with the at least one computer processor are also provided. The application server is configured to communicate with the web server and the database server for processing requests. The processing of requests including formulating system commands in response to the requests. A communication link is configured to connect the application server and the one or more computer managed openings for communication therebetween. The communication includes system commands which modify operation of the one or more computer managed openings. A method of managing is also presented.

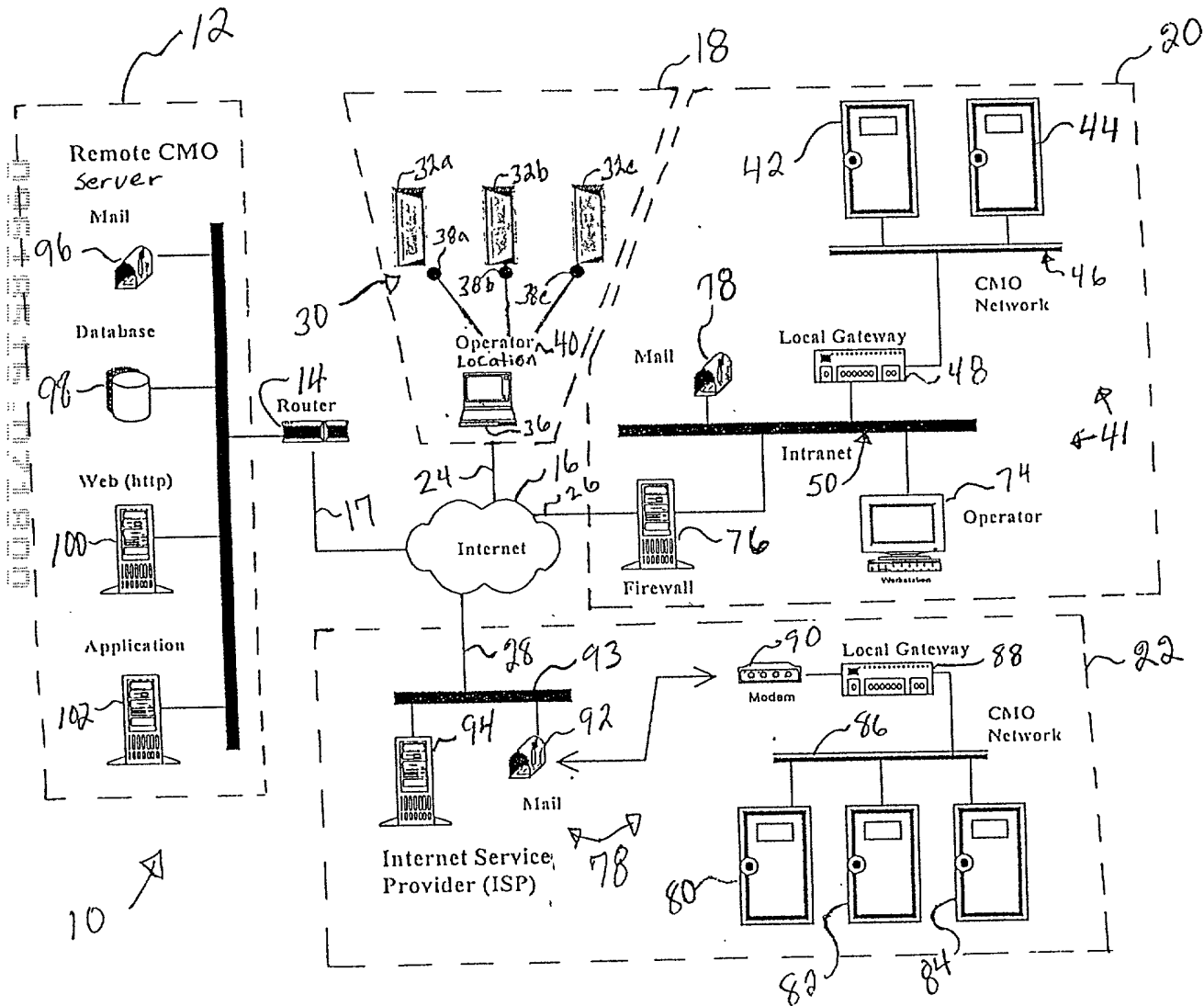


FIGURE 1

The diagram shows a network node 46, which is a rectangular box containing several internal components. On the left, a box labeled "Devices" 72 is connected to the node via a bidirectional arrow 52. Inside the node, there is a dashed-line boundary 70 enclosing the "Input / Output Ports" 54, "Non-volatile Memory for Database Storage" 60, "Clock" 64, "Reset" 66, "Service" 68, and "Transceiver" 62. Below this boundary is the "Micro-Processor (CPU)" 56. At the bottom of the node is a "Power Supply" 68. To the right of the node is a vertical bar labeled "COMMON NETWORK" 40. A vertical box labeled "LOCAL GATEWAY" 48 is connected to the network bar. The node 46 is connected to the network bar via a bidirectional arrow.

FIGURE 2

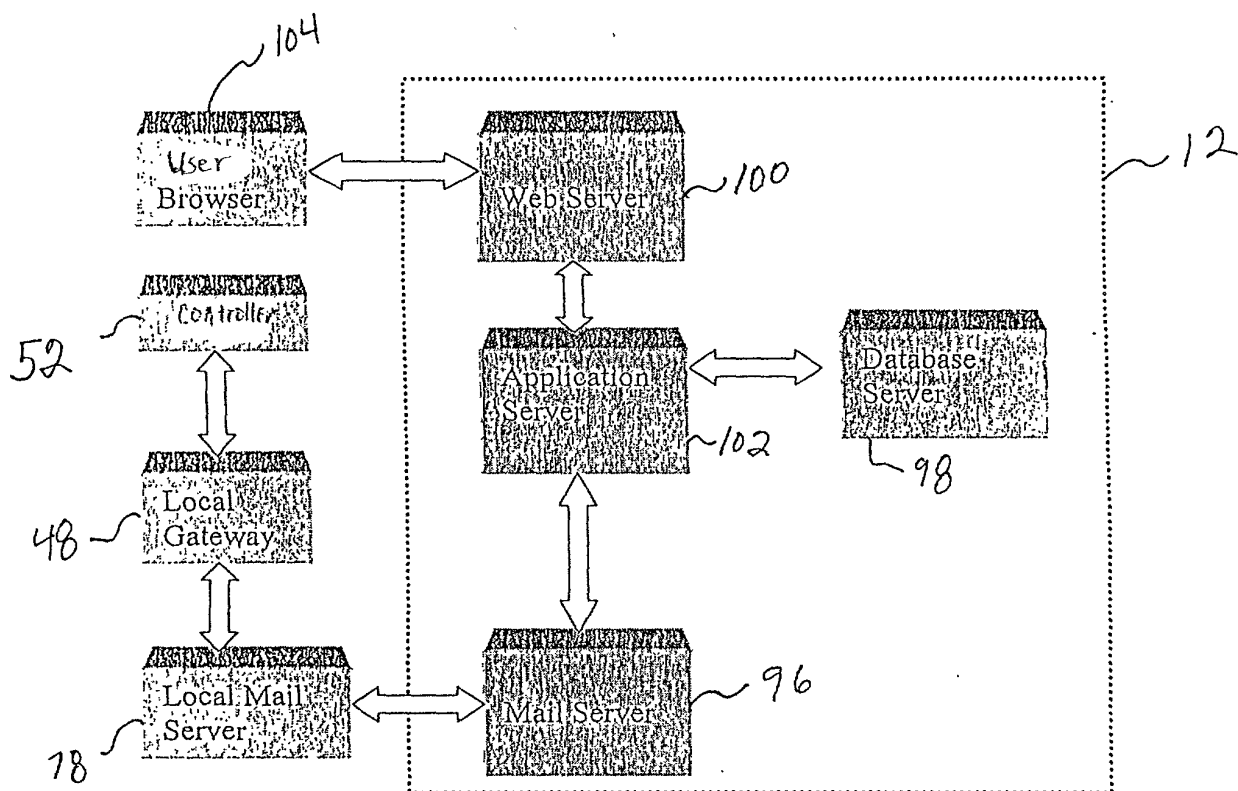
[illegible]

FIGURE 3

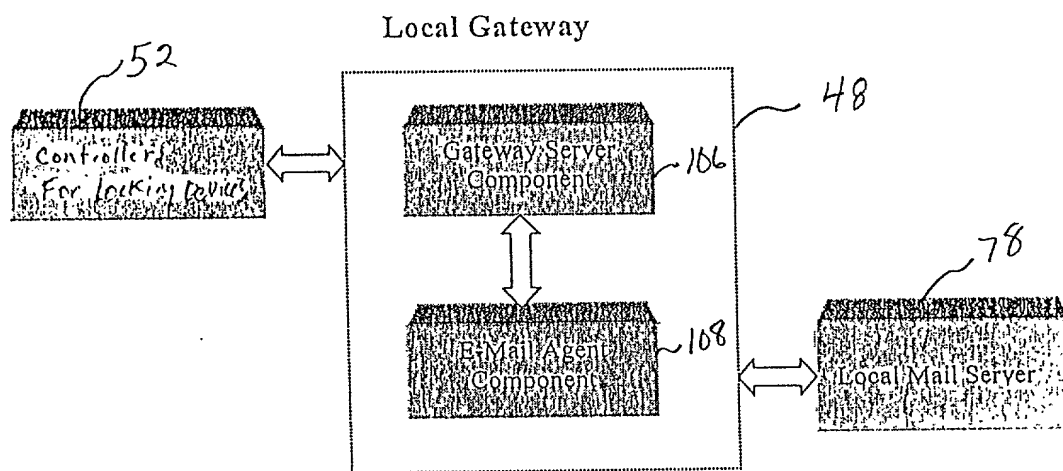
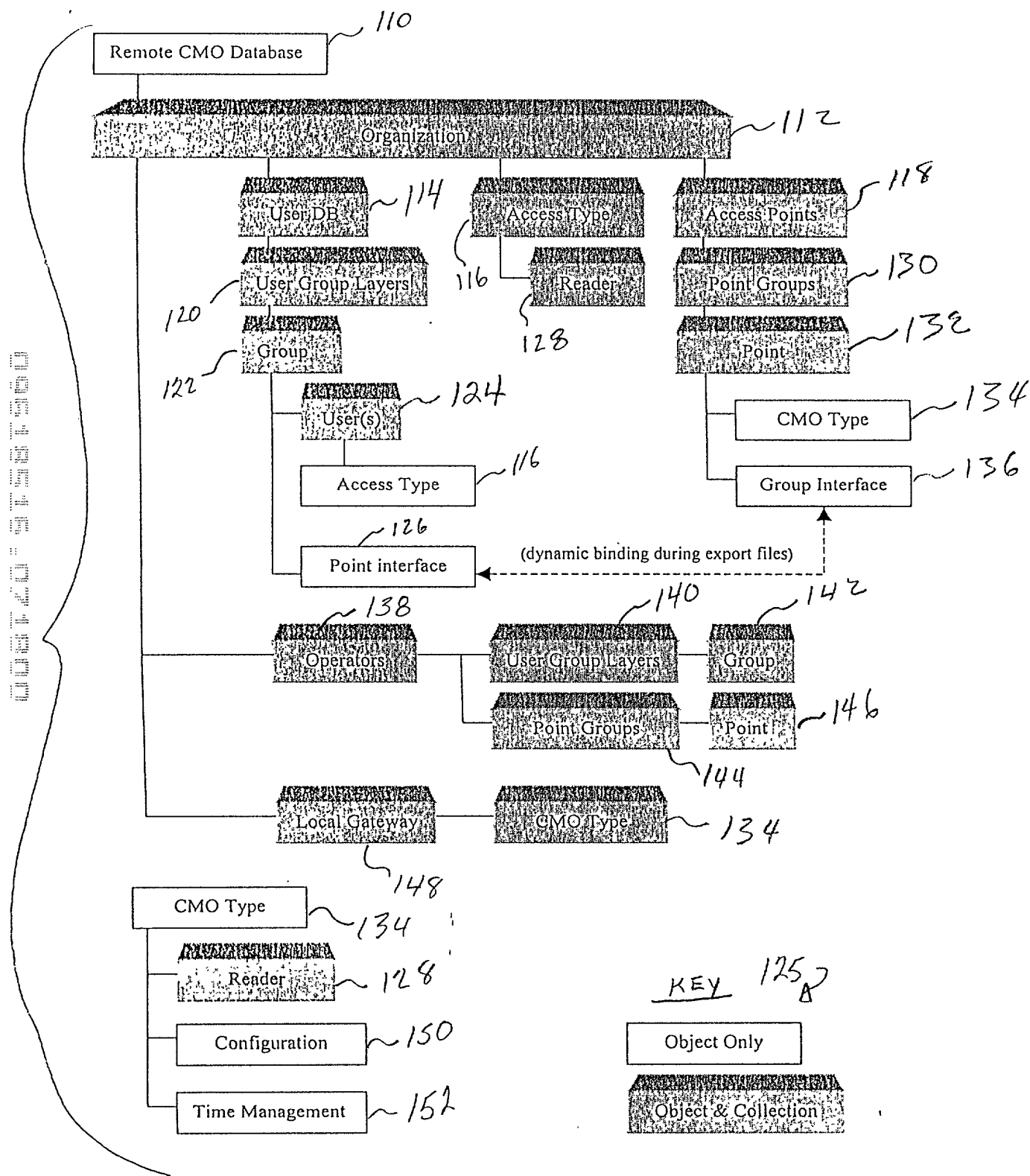


FIGURE 4



0010/PTO Rev. 6/95 DECLARATION <input checked="" type="checkbox"/> Declaration Submitted with Initial Filing OR <input type="checkbox"/> Declaration Submitted after Initial Filing	U.S. Department of Commerce Patent and Trademark Office		Attorney Docket Number	LOCK/170/US
			First Named Inventor	Gary E. Lavelle
	COMPLETE IF KNOWN			
	Application Number			
	Filing Date			
	Group Art Unit			
	Examiner Name			

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Internet Based Access Point Management System

(Title of the Invention)

the specification of which

☒ is attached hereto

OR

☐ was filed on (MM/DD/YYYY) _____ as United States Application or PCT International Application Number _____ and was amended on (MM/DD/YYYY) _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37 Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code §119 (a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Copy Attached? Yes No
None			<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

☐ Additional foreign application numbers are listed on a supplemental priority sheet attached hereto:

I hereby claim the benefit under Title 35, United States Code §119(e) of any United States provisional application(s) listed below:

Application Number(s)	Filing Date (MM/DD/YYYY)	<input type="checkbox"/> Additional provisional application numbers are listed on a supplemental priority sheet attached hereto.
None		

DECLARATION

Page 2

I hereby claim the benefit under Title 35, United States Code §120 of any United States application(s), or §365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations §1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. Parent Application Number	PCT Parent Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number (if applicable)
None			

☐ Additional U.S. or PCT international application numbers are listed on a supplemental priority sheet attached hereto.

As a named inventor, I hereby appoint the registered practitioners associated with the Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith, and direct that all correspondence be addressed to that Customer Number:

Firm Name: Alix, Yale & Ristas, LLP

Customer Number 002543

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name of Sole or First Inventor

☐ A petition has been filed for this unsigned inventor

Given Name	Gary	Middle Initial	E.	Family Name	Lavelle	Suffix	
Inventor's Signature	<i>Gary E. Lavelle</i>				Date	7-14-00	
RESIDENCE: City	Avon	State	CT	Country	U.S.A.	Citizenship	U.S.A.
POST OFFICE ADDRESS	485 Lovely Street						
City	Avon	State	CT	Zip	06001	Country	U.S.A.
						Applicant Authority	

Name of Additional Joint Inventor, if any:

☐ A petition has been filed for this unsigned inventor

Given Name	James	Middle Initial	C.	Family Name	Yuan	Suffix	
Inventor's Signature	<i>James C. Yuan</i>				Date	July 10, 2000	
RESIDENCE: City	San Jose	State	CA	Country	U.S.A.	Citizenship	U.S.A.
POST OFFICE ADDRESS	1537 Cameo Drive						
City	San Jose	State	CA	Zip	95129	Country	U.S.A.
						Applicant Authority	

☐ Additional inventors are being named on supplemental sheet(s) attached hereto.